

信息安全漏洞周报

2014 年 7 月 14 日-2014 年 7 月 20 日

2014 年第 29 期

本周漏洞基本情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 131 个，其中高危漏洞 30 个、中危漏洞 89 个、低危漏洞 12 个。上述漏洞中，可利用来实施远程攻击的漏洞有 118 个。本周收录的漏洞中，已有 90 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。本周互联网上出现“Frog CMS file_manager 插件任意文件上传漏洞”、“WordPress BSK PDF Manager 插件'wp-admin/admin.php' SQL 注入漏洞”等零日攻击代码，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 6 家成员单位、合作伙伴及个人报送了本周收录的全部 131 个漏洞。报送情况如表 1 所示。其中，安天实验室、启明星辰、奇虎 360、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、习科网络安全及白帽子向 CNVD 提交了 141 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
安天实验室	174	0
启明星辰	136	0
奇虎 360	96	96
恒安嘉新	90	0
绿盟科技	62	0

天融信	61	0
习科网络安全	9	9
High-Tech Bridge Security Research	1	1
CNCERT 山西分中心	15	15
CNCERT 山东分中心	6	6
CNCERT 江西分中心	3	3
CNCERT 青海分中心	2	2
CNCERT 吉林分中心	2	2
CNCERT 湖南分中心	2	2
CNCERT 河北分中心	1	1
CNCERT 内蒙古分中心	1	1
个人	3	3
报送总计	664	141
录入总计	131（去重）	141

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、WordPress、HP 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Oracle	31	24%
2	WordPress	23	18%
3	HP	7	5%
4	Cisco	7	5%
5	Juniper	6	5%
6	Drupal	5	4%
7	Google	3	2%
8	PHP	3	2%
9	Linux	1	1%
10	其他	45	34%

表 2 漏洞产品涉及厂商分布统计表

本周，CNVD 收录了 131 个漏洞。其中应用程序漏洞 69 个，WEB 应用漏洞 39 个，操作系统漏洞 11 个，网络设备漏洞 9 个，安全产品漏洞 2 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	69
WEB 应用漏洞	39
操作系统漏洞	11
网络设备漏洞	9
安全产品漏洞	2
数据库漏洞	1

表 3 漏洞按影响类型统计表

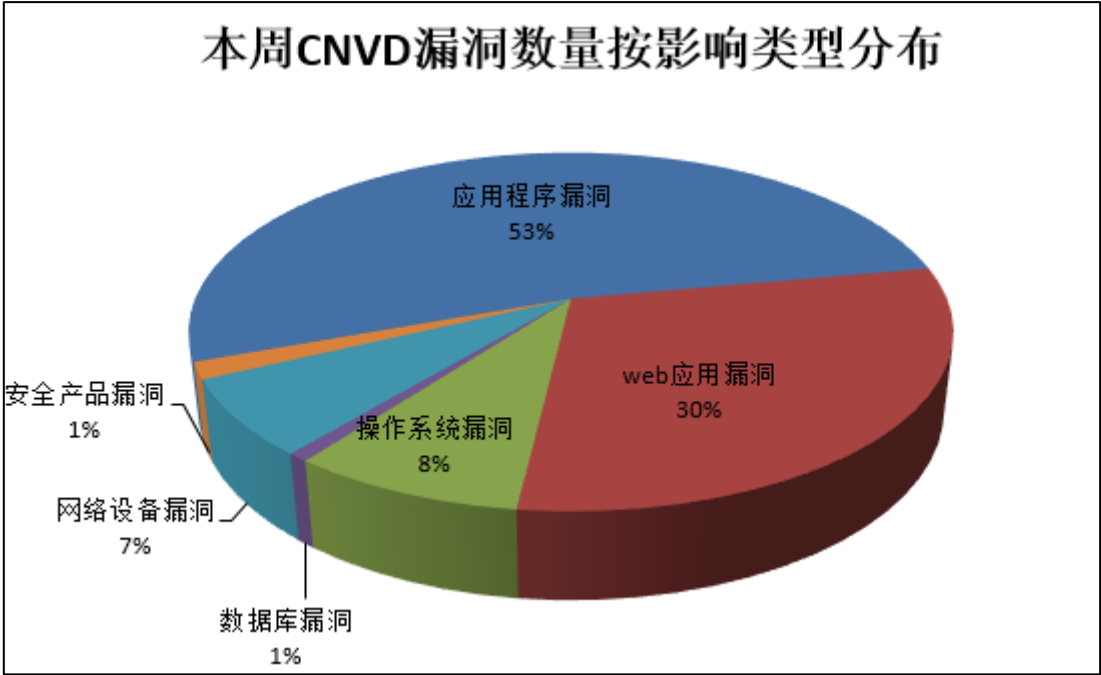


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 10 个电信行业漏洞，1 个移动互联网漏洞（如下图表所示）。其中，“Juniper SRX Junos 拒绝服务漏洞（CNVD-2014-04273、CNVD-2014-04271）”的综合评级均为“高危”。相关厂商已经发布了上述漏洞的修补程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2014-04252	Cisco Unified Communications Manager 目录遍历漏洞（CNVD-2014-04252）	中	否
电信	CNVD-2014-04251	Cisco Unified Communications Manager 目录遍历漏洞（CNVD-2014-04251）	中	否
电信	CNVD-2014-04250	Cisco Unified Communications Manager 任意文件上传漏洞	中	否

电信	CNVD-2014-04249	Cisco WebEx Meetings Server 和 WebEx Meeting Center 栈缓冲区溢出漏洞	中	否
电信	CNVD-2014-04248	Cisco WebEx Meetings 客户端任意文件下载漏洞	中	否
电信	CNVD-2014-04276	Juniper SRX Junos 拒绝服务漏洞 (CNVD-2014-04276)	中	是
电信	CNVD-2014-04273	Juniper SRX Junos 拒绝服务漏洞 (CNVD-2014-04273)	高	是
电信	CNVD-2014-04271	Juniper SRX Junos 拒绝服务漏洞 (CNVD-2014-04271)	高	是
电信	CNVD-2014-04308	Cisco Unified Communications Manager Real-Time Monitoring Tool 目录遍历漏洞	中	否
电信	CNVD-2014-04351	MongoDB 远程拒绝服务漏洞	中	是
移动互联网	CNVD-2014-04254	Google Android NFC 蓝牙简单配对消息拒绝服务漏洞	低	是

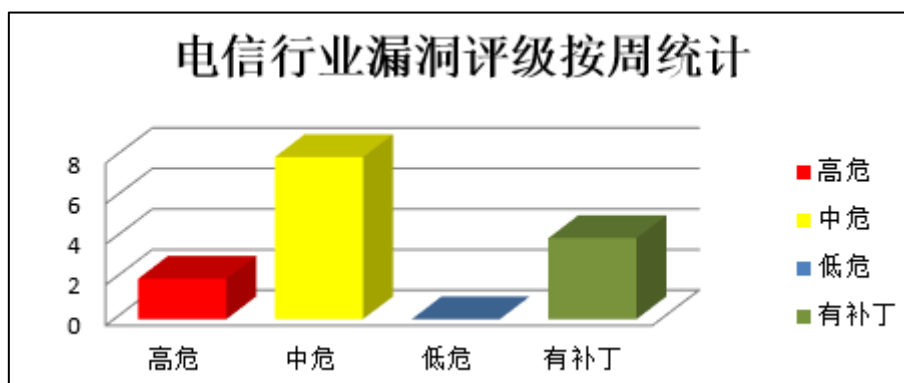


图 1 电信行业漏洞统计

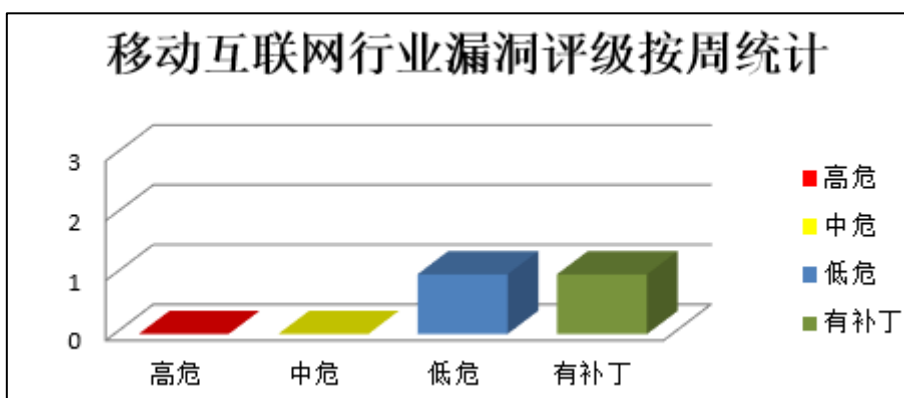


图 2 移动互联网行业漏洞统计

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Oracle 产品安全漏洞

7 月 15 日，Oracle 发布了 2014 年 7 月份的安全更新，修复了其多款产品存在的 114 个安全漏洞。受影响的产品包括：Oracle 数据库（5 个）、中间件产品 Fusion Middleware（29 个）、电子商务套装软件 Oracle E-Business Suite（5 个）、供应链套装软件 Oracle Supply Chain Products Suite（3 个）、企业管理器网格控制产品 Oracle Enterprise Manager Grid Control（1 个）、Oracle Siebel 托管型 CRM 软件（6 个）、Virtualization（15 个）、Hyperion（7 个）、PeopleSoft 产品（5 个）、Retail Applications（3 个）、Communications Applications（1 个）、Java SE（20 个）、Oracle 和 Sun 系统产品（4 个）和 MySQL 数据库（10 个）。

CNVD 收录的相关漏洞包括：Oracle Java SE JavaFX 子件任意代码执行漏洞、Oracle Java SE Libraries 子件任意代码执行漏洞、Oracle Java SE Hotspot 子件任意代码执行漏洞、Oracle Java SE 存在未明漏洞（CNVD-2014-04325、CNVD-2014-04324）。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/webinfo/show/3471>

2、HP 产品安全漏洞

HP Intelligent Management Center（iMC）是美国惠普（HP）公司的一套网络智能管理中心解决方案。Branch Intelligent Management System（BIMS）是其中的一个可对广域网中的客户端设备提供远程管理的软件模块。本周，上述产品被披露存在信息泄露漏洞，攻击者可利用漏洞修改数据或获取敏感信息。

CNVD 收录的相关漏洞包括：HP Intelligent Management Center 和 Branch Intelligent Management System 信息泄露漏洞（CNVD-2014-04365、CNVD-2014-04364、CNVD-2014-04363、CNVD-2014-04362、CNVD-2014-04361）。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04365>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04364>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04363>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04362>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04361>

3、Juniper 产品安全漏洞

Junos 是一款可靠的高性能网络操作系统。本周，上述产品被披露存在拒绝服务和权限提升漏洞，攻击者可利用漏洞发起拒绝服务攻击或提升权限。

CNVD 收录的相关漏洞包括：Juniper SRX Junos 拒绝服务漏洞（CNVD-2014-04271、CNVD-2014-04273、CNVD-2014-042736）、Juniper Junos 权限提升漏洞、Juniper Ju

nos 拒绝服务漏洞。除“Juniper SRX Junos 拒绝服务漏洞（CNVD-2014-04276）”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04271>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04273>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04276>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04272>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04274>

4、Cisco 产品安全漏洞

Cisco Adaptive Security Appliances(ASA, 自适应安全设备)是美国思科（Cisco）公司的一套防火墙设备。Cisco Unified Communications Manager (CUCM, Unified CM) 是美国思科（Cisco）公司的一款统一通信系统中的呼叫处理组件。Cisco WebEx Meetings Server 和 Cisco WebEx Meeting Center 都是美国思科（Cisco）公司的 WebEx 会议解决方案中的网络在线会议产品。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞读取任意文件，发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Cisco Adaptive Security Appliances 拒绝服务漏洞（CNVD-2014-04315）、Cisco Unified Communications Manager Real-Time Monitoring Tool 目录遍历漏洞、Cisco WebEx Meetings 客户端任意文件下载漏洞、Cisco WebEx Meetings Server 和 WebEx Meeting Center 栈缓冲区溢出漏洞、Cisco Unified Communications Manager 任意文件上传漏洞。其中“Cisco Adaptive Security Appliances 拒绝服务漏洞”厂商已经发布了修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04315>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04308>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04248>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04249>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04250>

5、InvGate Service Desk 存在多个 SQL 注入漏洞

InvGate Service Desk 是美国 InvGate 公司的一套基于 Web 且用于管理、分析和自动化 IT 服务支持的服务台软件。本周，InvGate Service Desk 被披露存在综合评级为“高危”的多个 SQL 注入漏洞。攻击者可以利用漏洞控制应用程序，访问或修改数据库数据。目前，厂商尚未发布该漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04260>

更多高危漏洞如表 3 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。

参考链接：<http://www.cnvd.org.cn/flaw/list.htm>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2014-04257	ArtifectxxClassified SQL 注入漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://xclassified.artifectx.com/
CNVD-2014-04313	RubyGemsbrbackup 存在多个漏洞	高	暂无
CNVD-2014-04283	WordPress 插件 WP Rss Poster SQL 注入漏洞	高	暂无
CNVD-2014-04279	WordPress BSK PDF Manager 插件'wp-admin/admin.php' SQL 注入漏洞	高	暂无
CNVD-2014-04288	Microsoft Internet Explorer 内存破坏漏洞（CNVD-2014-04288）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://technet.microsoft.com/library/security/ms14-018
CNVD-2014-04293	Infoblox Network Automation 产品 OS 命令注入漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.infoblox.com/en/products/netmri.html
CNVD-2014-04305	OpenVPNPrivateTunnel 'ptservice' 本地任意代码执行漏洞	高	暂无
CNVD-2014-04306	WordPress Download Manager 插件任意文件上传漏洞	高	暂无
CNVD-2014-04309	Raritan PX DPXR20A-16 认证绕过漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://www.raritan.net.cn/
CNVD-2014-04319	Aruba Networks ClearPass SQL 注入漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.arubanetworks.com/products/clearpass/guest/ http://www.arubanetworks.com/support/alerts/aid-07032014.txt

表 3 部分高危漏洞列表

小结：本周， Oracle 发布了 2014 年 7 月份的安全更新，修复了其多款产品存在的 11 4 个安全漏洞。受影响的产品包括：Oracle 数据库（5 个）、中间件产品 Fusion Middleware（29 个）、Java SE（20 个）和 MySQL 数据库（10 个）等。此外，HP、Juniper、Cisco 多

款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码，获取敏感信息或发起拒绝服务攻击。另外，InvGate Service Desk 被披露存在一个高危零日漏洞。攻击者可以利用漏洞控制应用程序，访问或修改数据库数据。建议相关用户应随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、Microsoft 修补 Internet Explorer 产品漏洞

Microsoft Internet Explorer 是一款流行的 WEB 浏览器。

本周，Microsoft 修补了上述产品存在的内存破坏漏洞，避免远程攻击者利用漏洞构建特制 WEB 页，诱使用户解析，可使应用程序崩溃或执行任意代码。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/47433>

本周要闻速递

1. 甲骨文 7 月安全更新

据甲骨文 7 月安全公告介绍，本次更新修复了 5 枚 Oracle 数据库漏洞、29 枚 Oracle Fusion 中间件漏洞、7 枚 Oracle Hyperion 漏洞、以及 E-Business Suite、Siebel CRM、PeopleSoft、Oracle Retail Applications 和 Primavera 等套件。甲骨文官方也建议消费者、企业用户尽早部署这些安全更新。其中影响最大的为 Oracle Fusion 中间件产品，累计修复近 29 个补丁，其中的 27 个漏洞通过网络可以无需验证进行攻击。受影响的中间件组件包括 BI Publisher、GlassFish Server、HTTP Server、JDeveloper、WebCenter Portal 和 WebLogic Server。另外，Java 安全更新修复了 20 枚远程漏洞，MySQL 数据库也迎来 10 枚安全补丁，修复其中两枚远程攻击安全问题。

参考链接：<http://soft.zol.com.cn/467/4675691.html>

2. 特斯拉存安全漏洞可变“遥控车”

在人们对隐私问题日益关注之际，苹果公司再度被推上了风口浪尖。日前，央视对苹果手机可搜集记录用户位置的功能提出质疑，认为苹果手机详细记录了用户位置和移动轨迹，并记录在未加密数据库中。而后，7 月 15 日，某公司公开表示，发现特斯拉汽车应用程序流程存在设计缺陷，攻击者利用这个漏洞，可远程控制车辆，实现开锁、鸣笛、闪灯、开启天窗等操作。

参考链接：<http://stock.hexun.com/2014-07-16/166657544.html>

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999